


Releasing system as means of releasing functions

Patent number: EP0937845
Publication date: 1999-08-25
Inventor: LANGENBACH JULIA DR (DE)
Applicant: MEGAMOS F & G SICHERHEIT (DE)
Classification:
 - international: E05B49/00
 - european: B60R25/00; G07C9/00E4
Application number: EP19990100358 19990114
Priority number(s): DE19981007473 19980224

Also published as:

 EP0937845 (B1)

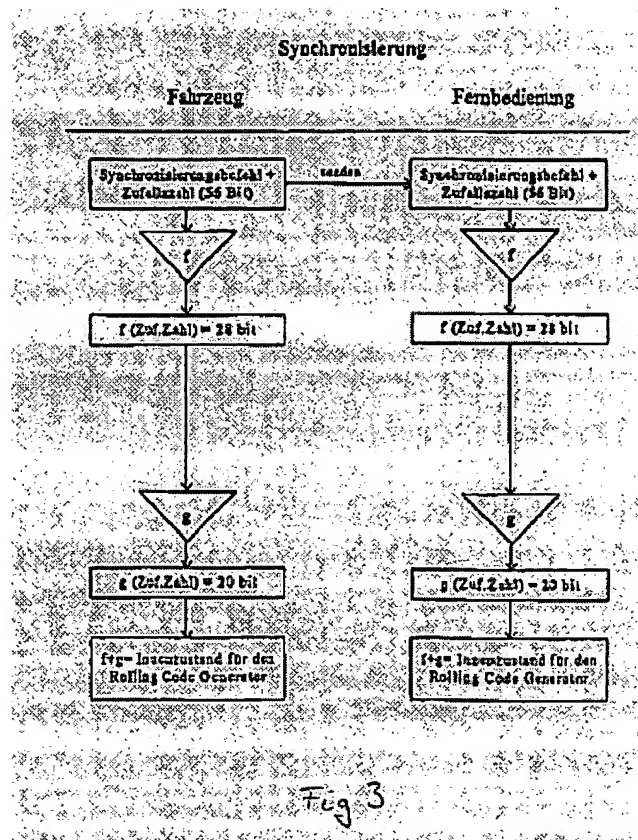
Cited documents:

 US5369706
 DE4428947
 US5646996

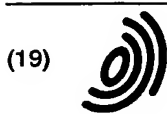
Report a data error here

Abstract of EP0937845

The system comprises a generator for gradually changing code outgoing from an internal condition. Comparison devices compare the code generated by the arrangement and a code received from the remote control. The internal conditions of the code generators are synchronized via a synchronization signal transmitted by the arrangement to the remote control. The release system examines whether a request for the release of functions of an arrangement is authorized. The remote control includes devices for transmitting the generated code over radio to the arrangement, as well as to a transponder which is suitable to authenticate the remote control to the arrangement.



Data supplied from the esp@cenet database - Worldwide



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 937 845 A1

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
25.08.1999 Patentblatt 1999/34

(51) Int. Cl.⁶: E05B 49/00

(21) Anmeldenummer: 99100358.3

(22) Anmeldetag: 14.01.1999

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(72) Erfinder: Langenbach, Julia,
Dr.
57258 Freudenberg (DE)

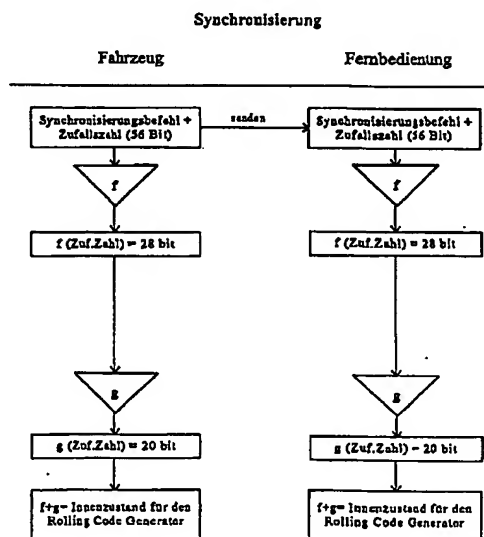
(74) Vertreter: Cohausz & Florack
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(30) Priorität: 24.02.1998 DE 19807473

(71) Anmelder:
f+g megamos Sicherheitselektronik GmbH
51674 Wiehl (DE)

(54) **Freigabesystem für die Freigabe von Funktionen einer Einrichtung**

(57) Die Erfindung betrifft ein Verfahren und ein Freigabesystem zur Überprüfung, ob eine Anforderung der Freigabe von Funktionen einer Einrichtung berechtigt ist, bei dem die Einrichtung und eine Fernbedienung jeweils einen Generator (6) aufweisen zum Erzeugen eines sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand, wobei die Fernbedienung des weiteren Mittel (3) umfaßt zum Übertragen des von ihr generierten Codes über Funkstrecke an die Einrichtung sowie einen Transponder (4), der geeignet ist, die Fernbedienung (2) gegenüber der Einrichtung zu authentifizieren, und wobei der Einrichtung Vergleichsmittel (7) zugeordnet sind zum Vergleichen des einrichtungsseitig generierten und des empfangenen Codes für eine Überprüfung der Berechtigung zur Freigabeanforderung. Für eine besonders günstige Neusynchronisierung der Innenzustände von Einrichtung und Fernbedienung ist vorgesehen, daß einrichtungsseitig Mittel (9) zum Bereitstellen eines Synchronisierungssignals sowie Ausgabemittel (9) zum Übertragen des Synchronisierungssignals an den Transponder (4) der Fernbedienung (2) vorgesehen sind, wobei die Innenzustände der Code Generatoren (5,6) mittels des Synchronisierungssignals miteinander synchronisierbar sind.



EP 0 937 845 A1

Beschreibung

[0001] Die Erfindung betrifft ein Freigabesystem zur Überprüfung, ob eine Anforderung der Freigabe von Funktionen einer Einrichtung berechtigt ist, wobei die Funktionen beispielsweise in der Entschärfung einer Alarmanlage oder einer Wegfahrsperre und in der Aktivierung einer Zentralverriegelung eines Fahrzeugs bestehen können, mit einem einrichtungsseitig angeordneten ersten Generator zum Erzeugen eines ersten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des ersten Generators, sowie mit einer Fernbedienung, die einen zweiten Generator umfaßt zum Erzeugen eines zweiten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des zweiten Generators, Mittel zum Übertragen des generierten zweiten Codes über eine Funkstrecke an die Einrichtung und einen Transponder, der geeignet ist, die Fernbedienung gegenüber der Einrichtung zu authentifizieren, wobei der Generator der Fernbedienung und der Generator der Einrichtung geeignet sind zur synchronen Generierung eines Codes und wobei dem einrichtungsseitigen ersten Generator Vergleichsmittel zugeordnet sind zum Vergleichen des einrichtungsseitig generierten und des in der Fernbedienung generierten und zu der Einrichtung übertragenen Codes für eine Überprüfung der Berechtigung der Fernbedienung zur Anforderung der Freigabe der Funktionen. Die Erfindung betrifft ebenso ein Verfahren bezüglich eines solchen Freigabesystems.

[0002] Aus der Praxis ist der Einsatz von Fernbedienungen bekannt, die einer geeignet ausgebildeten Einrichtung eines Fahrzeugs über eine Funkstrecke Berechtigungsinformationen für die kontrollierte Freigabe von Fahrzeugfunktionen liefern. Die so überwachten Fahrzeugfunktionen können die Entschärfung der Alarmanlage, die Freigabe der Wegfahrsperre und/oder die Aktivierung der Zentralverriegelung umfassen. Die eingesetzten Berechtigungsinformationen bestehen aus einem Wert, der geeignet ist, die Fernbedienung dem Fahrzeug gegenüber zu identifizieren und als zur Anforderung einer Freigabe der Fahrzeugfunktionen berechtigt auszuweisen.

[0003] Die zu diesem Zweck ursprünglich eingesetzten Festcode-Verfahren, nach denen die Information, die von einer Fernbedienung übertragen wird, zwar gerätespezifisch aber für eine Fernbedienung festgelegt ist, sind sehr unsicher, da bei jeder Kommunikation die gleiche Information gesendet wird. Dadurch kann die Information von einem Unbefugten abgehört, aufgenommen und zu einer Freigabe der Fahrzeugfunktionen verwendet werden.

[0004] Aus diesem Grund werden heute zunehmend sogenannte "Rolling Code"-Verfahren eingesetzt. Diese Rolling Code-Verfahren zeichnen sich im Gegensatz zu den Festcode-Verfahren dadurch aus, daß bei jeder Übertragung einer Berechtigungsinformation ein anderer Wert als Rolling Code gesendet wird, der nur einmal

verwendbar ist.

[0005] Als zu übertragender Wert wird in der Regel eine binäre Zahl verwendet, die sich jedesmal ändert und die jedesmal wie zufällig aussieht. Wirklich zufällig kann die Zahl allerdings nicht sein, da das Fahrzeug zur Überprüfung wissen muß, welcher Wert von der berechtigten Fernbedienung zu erwarten ist. Zu Gewährleistung einer hohen Sicherheit bestehen deshalb die Hauptanforderungen bei solchen Verfahren darin, daß die Zahl lang genug sein muß, daß sie sich nie wiederholen darf und daß sie auch nicht vorhersagbar sein darf.

[0006] Es existieren unterschiedliche kryptographische Verfahren für die Erzeugung von Rolling Codes. Zum einen kann ein Zähler eingesetzt werden, dessen jeweils aktueller Stand verschlüsselt wird, oder aber es wird ausgehend von dem letzten Rolling Code mittels eines Algorithmus eine "Zufallszahl" erzeugt.

[0007] Sowohl in der Fernbedienung als auch in dem Fahrzeug ist jeweils ein Generator zur Erzeugung der Rolling Codes integriert. Damit das Fahrzeug in der Lage ist, einen von der Fernbedienung erhaltenen Rolling Code zu verifizieren, müssen die Generatoren identisch sein und sich im gleichen Zustand befinden, also synchron laufen. Die Sicherheit des Systems basiert in der Regel auf einer Geheimzahl, dem Secret Key, die nur dem Fahrzeug und der Fernbedienung bekannt ist. Der interne Zustand der Generatoren ist für einen externen Beobachter ebenfalls unbekannt. Die Geheimhaltung dieses Zustandes ist einer der sicherheitsrelevanten Aspekte des Systems.

[0008] Hieraus können sich in der praktischen Anwendung Probleme ergeben. So weist die Fernbedienung eine Batterie auf, die irgendwann leer ist. Das System darf in diesem Fall kein Reset durchführen und in den Ursprungszustand zurückkehren, denn das würde bedeuten, daß die Zahlen, die schon einmal übertragen worden sind, sich wiederholen würden und das Fahrzeug sie akzeptieren müßte. Das heißt, daß ein Memory vorhanden sein muß, in dem der aktuelle Zustand nach jeder Übertragung gespeichert wird. Normalerweise wird als Memory ein EEPROM eingesetzt. Das führt aber zu einer Reduzierung der Lebensdauer der Fernbedienung, da ein EEPROM nur begrenzt beschreibbar ist, meistens bis zu 10 000 mal.

[0009] Das Schreiben muß ferner da erfolgen, wo das Fahrzeug sich gerade befindet. Das bedeutet eventuelle Störungen und als Ergebnis falsche Werte im EEPROM. In schlimmsten Fall kann der ganze Inhalt des EEPROM verloren gehen, und die Fernbedienung muß neu programmiert oder ersetzt werden.

[0010] Außerdem kann die Synchronisierung verloren gehen, wenn der Benutzer in Abwesenheit des Fahrzeugs auf den Senderknopf drückt.

[0011] Es gibt zur Zeit unterschiedliche Verfahren, die Synchronisierung wiederherzustellen. Eine Möglichkeit besteht darin, die Neusynchronisierung in einer Werkstatt durchführen zu lassen. Dies ist jedoch für den Nut-

zer des Fahrzeugs unpraktisch und teuer. Es sind zudem Möglichkeiten bekannt, um im Auto neu zu synchronisieren. Diese sind zwar praktischer und billiger für den Nutzer, führen aber zu hohen Sicherheitseinbußen. Die hierzu eingesetzten Verfahren basieren darauf, daß mindestens zwei aufeinanderfolgende Rolling Codes hintereinander über die Funkstrecke von der Fernbedienung an das Fahrzeug übertragen werden. Erweist sich nun im Fahrzeug, daß der zweite Rolling Code aus dem ersten mittels des eingesetzten kryptographischen Verfahrens zur Erzeugung der Rolling Codes generiert werden konnte, so wird er als neuer Innenzustand für den Code Generator des Fahrzeugs akzeptiert. Da der erste Rolling Code mehr oder weniger beliebig sein kann, wird auch eine beliebige Anzahl an möglichen Kombinationen von Rolling Codes akzeptiert.

[0012] Aufgrund dieser großen Anzahl möglicher Codepaare ist es aber bei Kenntnis eines Teils des kryptographischen Algorithmus meistens wesentlich einfacher, ein gültiges Rolling Code Paar zu finden, als eine einzige richtige Zahl, so daß das Risiko eines unberechtigten Neusetzens des Innenzustandes des Codegenerators im Fahrzeug gegeben ist.

[0013] Eine Fernbedienung für die Freigabe von Fahrzeugfunktionen unter Einsatz des Rolling Code Verfahrens wird in der Druckschrift DE 44 28 947 C1 beschrieben. Basierend auf dem aktuellen Zustand eines Codetaktimpulsgenerators in der Fernbedienung wird ein Rolling Code generiert und an das Fahrzeug gesendet. Dieses enthält ebenfalls einen Codetaktimpulsgenerator, dessen Zustand mit dem Zustand des Codetaktimpulsgenerator in der Fernbedienung synchronisiert ist. Dadurch kann im Fahrzeug bestimmt werden, welcher Wert von der berechtigten Fernbedienung zu erwarten ist, und nur bei Übereinstimmung des empfangenen Rolling Codes mit einem intern erzeugten Rolling Code erfolgt eine Freigabe der Fahrzeugfunktionen. In der Fernbedienung ist zusätzlich ein Transponder vorgesehen, mit dem eine Möglichkeit geschaffen wird, auch nach einem Ausfall des Energiespeichers im Sender über die Fernbedienung einen Zugang zu den geschützten Fahrzeugfunktionen zur Verfügung zu stellen. Zu diesem Zweck wird ein im Transponder gespeicherter Code auf Anfrage des Fahrzeugs hin zu diesem übertragen und dort anhand eines gespeicherten Wertes überprüft. Bei erfolgreicher Authentifizierung werden die Fahrzeugfunktionen freigegeben. Anschließend wird für die nächste Anfrage ein neuer Code einerseits im Fahrzeug gespeichert und andererseits an den Transponder übertragen und in dem Transponderspeicher abgelegt.

[0014] In der DE 44 28 947 C1 sind jedoch keine Maßnahmen vorgesehen für den Fall, daß die Synchronisierung zwischen dem Codeimpulsgenerator der Fernbedienung und dem Codeimpulsgenerator des Fahrzeugs aufgrund des Ausfalls des Energiespeichers der Fernbedienung oder aufgrund eines sonstigen Fehlers verloren gegangen ist.

[0015] Der Erfindung liegt die Aufgabe zugrunde, ein Freigabesystem zur Überprüfung der Berechtigung einer Anforderung der Freigabe von Fahrzeugfunktionen gemäß dem Oberbegriff sowie ein Verfahren für eine solche Überprüfung zur Verfügung zu stellen, die eine sichere und wenig aufwendige Neusynchronisierung der Rolling Code Generatoren in Fahrzeug und Fernbedienung ermöglichen.

[0016] Die Erfindung wird zum einen bei einem Freigabesystem gemäß dem Oberbegriff des Anspruchs 1 dadurch gelöst, daß einrichtungsseitig Mittel zum Bereitstellen eines Synchronisierungssignals sowie Ausgabemittel zum Übertragen des Synchronisierungssignals an den Transponder der Fernbedienung vorgesehen sind, wobei die Innenzustände der Code Generatoren mittels des Synchronisierungssignals miteinander synchronisierbar sind.

[0017] Zum anderen wird die Erfindung gelöst durch ein Verfahren für ein Freigabesystem zur Überprüfung, ob eine Anforderung der Freigabe von Funktionen einer Einrichtung berechtigt ist, wobei die Funktionen beispielsweise in der Entschärfung einer Alarmanlage oder einer Wegfahrsperre und in der Aktivierung einer Zentralverriegelung eines Fahrzeugs bestehen können, mit einem einrichtungsseitig angeordneten ersten Generator zum Erzeugen eines ersten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des ersten Generators, sowie mit einer Fernbedienung, die einen zweiten Generator umfaßt zum Erzeugen eines zweiten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des zweiten Generators, Mittel zum Übertragen des generierten zweiten Codes über eine Funkstrecke an die Einrichtung und einen Transponder, der geeignet ist, die Fernbedienung gegenüber der Einrichtung zu authentifizieren, wobei der Generator der Fernbedienung und der Generator der Einrichtung geeignet sind zur synchronen Generierung eines Codes und wobei dem einrichtungsseitigen ersten Generator Vergleichsmittel zugeordnet sind zum Vergleichen des einrichtungsseitig generierten und des in der Fernbedienung generierten und zu der Einrichtung übertragenen Codes für eine Überprüfung der Berechtigung der Fernbedienung zur Anforderung der Freigabe der Funktionen, und wobei das Verfahren die folgenden Schritte umfaßt:

- Senden eines Synchronisierungsbefehls, insbesondere eines Headers, von der Einrichtung an den Transponder der Fernbedienung zum Signalisieren, daß neu synchronisiert werden soll,
- Senden einer Zufallszahl von der Einrichtung an den Transponder der Fernbedienung und
- Speichern eines auf der Zufallszahl basierenden Wertes als aktuellen Innenzustand der beiden Generatoren in Einrichtung und Fernbedienung.

[0018] Durch das erfindungsgemäße Freigabesystem

und das erfindungsgemäße Verfahren wird ein Nachsynchronisieren ohne zusätzlichen Aufwand bei gleichzeitiger Wahrung einer hohen Sicherheit ermöglicht, indem der ohnehin in der Fernbedienung vorhandene Transponder zusätzlich als Empfänger für ein Synchronisierungssignal genutzt wird. Die Nachsynchronisierung erfolgt automatisch, so daß keine spezielle und aufwendige Nachsynchronisierung bei verlorengegangener Synchronisierung erforderlich ist. Die neue Synchronisierung soll jedoch erst dann erfolgen, wenn sich die Fernbedienung über den Transponder authentifiziert hat oder sich durch den Vergleich der generierten Rolling Codes als berechtigt erwiesen hat. Während des gesamten Ablaufs bleibt der innere Zustand der Code Generatoren für einen externen Beobachter völlig unbekannt.

[0019] Hinzu kommt, daß das Schreiben in ein EEPROM nicht mehr notwendig ist. Unter normalen Umständen sind die aktuellen Zustandswerte in einem Memory gespeichert.

[0020] Die von der Einrichtung generierte und an den Transponder der Fernbedienung übersandte Zufallszahl wird vorzugsweise zunächst sowohl in der Einrichtung als auch in der Fernbedienung mit der gleichen Verschlüsselungsfunktion verschlüsselt, bevor sie zum Setzen der aktuellen Innenzustände der Code Generatoren in Einrichtung und Fernbedienung verwendet wird, da so eine besonders große Sicherheit erzielt werden kann.

[0021] Vorteilhafterweise sendet die Fernbedienung nicht nur einen jeweils geänderten Code an die Einrichtung, sondern zusätzlich einen Festcode, der sich aus Werten wie ID-Nummer, Header und Knopffunktion zusammensetzt.

[0022] Besonders günstig kann die Synchronisierung ausgeführt werden, wenn die Synchronisierungssignale, die die Einrichtung an den Transponder der Fernbedienung sendet, sich zusammensetzen aus einem Synchronisierungsbefehl, der der Fernbedienung bekannt gibt, daß neu synchronisiert werden soll, und einer Zufallszahl, die verwendet wird um den neuen Innenzustand des Code Generators der Fernbedienung zu setzen.

[0023] Nach einer bevorzugte Möglichkeit der Authentifizierung des Transponder sendet zunächst die Einrichtung eine Zufallszahl und eine mit der Funktion f verschlüsselte Zufallszahl an den in der Fernbedienung integrierten Transponder. Der Transponder empfängt die Zufallszahl, verschlüsselt sie und vergleicht sie mit der empfangenen verschlüsselten Zufallszahl. Falls sich eine Übereinstimmung ergibt, so wird die Zahl weiter verschlüsselt, diesmal mit der Funktion g, und zurück an die Einrichtung übertragen. Die Einrichtung prüft das Ergebnis und erkennt den Transponder als gültig an oder lehnt ihn ab. Auf diese Weise wird zunächst die Einrichtung gegenüber der Fernbedienung authentifiziert und anschließend die Fernbedienung gegenüber der Einrichtung, so daß eine besonders hohe Sicherheit

vor Manipulationen gegeben ist.

[0024] Die gleichen geheimen Funktionen f und g können auch von Fernbedienung und Einrichtung verwendet werden, um die mit einem Synchronisierungssignal übermittelte Zufallszahl zu verschlüsseln, bevor sie für das Setzen des neuen, synchronisierten Innenzustands der Code Generatoren in Fernbedienung und Einrichtung verwendet werden.

[0025] Das erfindungsgemäße Freigabesystem und das erfindungsgemäße Verfahren für ein Freigabesystem können vorteilhaft für die Synchronisierung beliebiger, in Einrichtung und Fernbedienung verwendeter Code Generatoren, die sich ändernde, aber aufeinander abgestimmte Codes erzeugen sollen, eingesetzt werden. Vorzugsweise ist das Freigabesystem jedoch mit Rolling Code Generatoren versehen, die jedesmal einen anderen, sich nie wiederholenden Rolling Code zur Verfügung stellen. Durch den Einsatz solcher Rolling Code Generatoren wird eine besonders hohe Sicherheit erzielt. Aber auch bei Rolling Code Systemen verbleibt eine gewisse "Vorhersagbarkeit" des Innenzustandes. Abhängig von der benutzten Kryptographie ist es schwieriger oder leichter, den nächsten Zustand zu erraten. Allen Systemen ist aber gemein, daß der neue Zustand aus dem vorherigen Zustand berechnet wird, so daß die Zahlen nicht wirklich zufällig sind.

[0026] Das erfindungsgemäße Freigabesystem kann nach einer weiteren bevorzugten Ausführungsform dazu eingesetzt werden, diese Schwachstelle der Rolling Code Systeme zu umgehen und eine erhöhte Sicherheit zu gewährleisten. Dies wird erreicht, indem eine neue Synchronisierung nach jeder erfolgreichen Berechtigungsprüfung über den Vergleich der Rolling Codes vorgesehen wird:

[0027] Der Rolling Code Generator der Fernbedienung hat einen bestimmten Innenzustand. Daraus wird ein Rolling Code generiert und dieser zu der Einrichtung gesendet. Falls der Code gültig ist, werden die gesicherten Funktionen freigegeben. Befindet sich nun der Transponder der Fernbedienung im Feld der Einrichtung, so wird wie weiter oben beschrieben "nachsynchronisiert", obwohl die vorherige Funkübertragung gültig war. Der Generator erhält somit einen neuen Innenzustand und kann einen neuen Rolling Code erzeugen. Die Innenzustände sind also nicht mehr sich aus dem jeweils letzten Innenzustand ergebende Zahlen; vielmehr "springen" sie nun "echt" zufällig im ganzen Zahlenraum.

[0028] Rolling Code Systeme arbeiten normalerweise mit einem sogenannten "Empfangsfenster". Das bedeutet, daß der Senderknopf der Fernbedienung auch in Abwesenheit der Einrichtung betätigt werden kann, ohne daß die Synchronisierung verloren geht. Die Anzahl der Knopfdrücke darf hierzu lediglich eine vorgegebene Zahl nicht überschreiten. Diese vorgegebene Zahl heißt "Fenstergröße". Das erfindungsgemäße Freigabesystem wird gemäß einer bevorzugten Ausführungsform

rungsform mit einem solchen Fenster kombiniert. Dadurch ist ein Nachsynchronisieren nur dann erforderlich, wenn die Fenstergröße überschritten wird.

[0029] Bei einer Kombination der Verwendung eines "Empfangsfensters" mit einer jedesmal erfolgenden "Nachsynchronisierung" wird der Zustand der Rolling Code Generatoren erst nach einer gültigen Übertragung "nachsynchronisiert". Das heißt, daß erst innerhalb des Fensters gesucht wird, ob der Rolling Code stimmt, und nur dann wird der Innenzustand durch die "Nachsynchronisierung" springen.

[0030] Weitere vorteilhaft Ausgestaltungen des erfindungsgemäßen Freigabesystems und des erfindungsgemäßen Verfahrens gehen aus den Unteransprüchen hervor.

[0031] Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels unter Bezugnahme auf Zeichnungen näher erläutert. Dabei zeigt

Fig. 1 ein Blockschaltbild eines Ausführungsbeispiels des erfindungsgemäßen Freigabesystems, eingesetzt zur Überwachung der Freigabe bestimmter Funktionen eines Fahrzeugs,

Fig. 2 ein Ablaufdiagramm, das die Signalübertragung zwischen der Fernbedienung und dem Fahrzeug verdeutlicht, und

Fig. 3 ein Ablaufdiagramm, in dem die Synchronisierung der Rolling Code Generatoren verdeutlicht wird.

[0032] In Figur 1 sind die wesentlichen Elemente eines erfindungsgemäßen Freigabesystems dargestellt, mit dem die Startfunktion eines Fahrzeuges kontrolliert freigegeben werden kann.

[0033] Das Freigabesystem umfaßt zur Ermöglichung einer solchen kontrollierten Freigabe eine Einrichtung in einem Fahrzeug 1 und eine Fernbedienung 2, die geeignet sind, miteinander zu kommunizieren.

[0034] Die Fernbedienung 2 weist hierzu zum einen Mittel 3 zum Übertragen von Informationen über Funkstrecke auf und zum anderen einen Transponder 4, der geeignet ist, ohne Bedarf an Energie aus der Fernbedienung 2 Signale von dem Fahrzeug zu empfangen und Signale an das Fahrzeug zu senden. Für die reguläre Authentifizierung der Fernbedienung 2 gegenüber dem Fahrzeug verfügt die Fernbedienung 2 über einen gespeicherten Festcode und weist einen Generator 5 auf, der einen jedesmal unterschiedlichen Rolling Code in Abhängigkeit von einem aktuellen Innenzustand erzeugt. Der Transponder 4 umfaßt ferner Mittel, die eine Verschlüsselung von Zahlen mit verschiedenen Funktionen f und g ermöglichen, sowie Vergleichsmittel zum Vergleichen empfangener Zahlen mit in der Fernbedienung 2 selbst verschlüsselten Zahlen.

[0035] Die Einrichtung des Fahrzeugs 1 weist Mittel 8 zum Empfangen von Funksignalen und mit Mitteln zum Bereitstellen von Synchronisierungssignalen versehene

Sende/Empfangsmitteln 9 zum Übertragen von Aktivierungsenergie und von Signalen an den Transponder 4 der Fernbedienung sowie zum Empfangen von vom Transponder 4 ausgesandten Signalen auf. Ebenso wie die Fernbedienung 2 hat die Einrichtung des Fahrzeugs 1 Zugriff auf einen gespeicherten Festcode, und sie umfaßt auch einen Generator 6 zum Erzeugen eines Rolling Codes in Abhängigkeit eines aktuellen Innenzustands und Vergleichsmittel 7 zum Vergleichen intern generierter Werte mit empfangenen Werten.

[0036] Mit den in Fernbedienung 2 und Fahrzeug bereitgestellten Elementen sind zwei separate Kommunikationsstrecken vorhanden. Die Funkstrecke, die zwischen den Übertragungsmitteln 3 der Fernbedienung 2 und dem Empfangsmitteln 8 des Fahrzeugs gegeben ist, ist unidirektional ausgebildet, nämlich von der Fernbedienung 2 zum Fahrzeug. Die Niedrigfrequenzstrecke zwischen dem Transponder 4 der Fernbedienung 2 und den Sende/Empfangsmitteln 9 des Fahrzeugs dagegen ist bidirektional, da der in der Fernbedienung 2 integrierte Transponder 4 Signale nicht nur senden sondern auch empfangen kann.

[0037] Über die Funkstrecke erfolgt die reguläre Freigabe der Fahrzeugfunktionen über ein Freigabesignal S nach einem Vergleich der von den Rolling Code Generatoren 5,6 von Fernbedienung 2 und Fahrzeug generierten Rolling Codes. Über die Niedrigfrequenzstrecke wird eine Authentifizierung der Fernbedienung 2 über den Transponder 4 für eine ersatzweise Freigabe der Fahrzeugfunktionen sowie eine neue Synchronisierung der Rolling Code Generatoren 5,6 ermöglicht.

[0038] In den Figuren 2 und 3 ist der Datenaustausch zwischen der Einrichtung des Fahrzeugs 1 und der Fernbedienung 2 sowie die Verarbeitung der Daten innerhalb des Fahrzeugs bzw. innerhalb der Fernbedienung 2 bei dem Einsatz eines erfindungsgemäßen Freigabesystems dargestellt.

[0039] Bezüglich einer Kommunikation zwischen Fernbedienung 2 und Fahrzeug sind mehrere Situationen, die sich ergeben können, zu berücksichtigen.

[0040] Zunächst einmal sei die in den Figuren 2 und 3 nicht einbezogene Situation gegeben, daß das Fahrzeug erkennt, daß sich ein gültiger Transponder 4 im Feld der Einrichtung des Fahrzeugs befindet, ohne daß ein Versuch erfolgt, mit der Fernbedienung 2 eine Kommunikation über die Funkstrecke aufzubauen. Der Start wird daraufhin im Rahmen einer "Notfunktion" freigegeben, da seitens des Fahrzeugs in diesem Fall angenommen wird, daß eine Kommunikation über Funkstrecke deshalb nicht erfolgte, weil die Batterie der Fernbedienung 2 leer ist.

[0041] Für die Überprüfung der Gültigkeit des Transponders 4 senden die Sende/Empfangsmittel 9 des Fahrzeugs eine Zufallszahl und eine mit der Funktion f verschlüsselte Zufallszahl an den in der Fernbedienung 2 integrierten Transponder 4. Der Transponder 4, der mit von dem Fahrzeug erhaltener Energie aktiviert wurde, empfängt die Zufallszahl, verschlüsselt sie und

vergleicht sie mit der empfangenen verschlüsselten Zufallszahl. Falls sich eine Übereinstimmung ergibt, so wird die Zahl weiter verschlüsselt, diesmal mit der Funktion g, und zurück an das Fahrzeug übertragen. Das Fahrzeug prüft das Ergebnis und erkennt den Transponder 4 als gültig an oder lehnt ihn ab. Eine spezielle weitere Reaktion des Fahrzeugs außer der Freigabe der kontrollierten Fahrzeugfunktionen ist hier nicht notwendig.

[0042] Die Funktionsweise des Freigabesystems in allen weiteren Situationen, bei denen zumindest irgendeine Information von einer Fernbedienung 2 über Funkstrecke an die Mittel 8 des Fahrzeugs zum Empfangen von Funksignalen übermittelt wird, wird im folgenden anhand der Figuren 2 und 3 erläutert.

[0043] Unter Einbezug ihres jeweiligen Innenzustands 1 bzw. 2 generieren die Code Generatoren 5 bzw. 6 von Fahrzeug und Fernbedienung 2 einen Rolling Code 1 bzw. 2 und die gespeicherten Festcodes 1 bzw. 2 werden ausgelesen. Die Fernbedienung 2 sendet nun seine Codeinformation an das Fahrzeug, in dem durch die Vergleichsmittel 7 überprüft wird, ob der von der Fernbedienung 2 empfangene Festcode 2 übereinstimmt mit dem Festcode 1 des Fahrzeug. Der Festcode umfaßt dabei ID-Nummer, Header und Knopffunktion.

[0044] Bei mangelnder Übereinstimmung der beiden Festcodes 1 und 2 wird die Anfrage ignoriert und das Verfahren abgebrochen. Ist ein gültiger Transponder 4 vorhanden, so wird über die bereits erwähnte "Notfunktion" der Start dennoch freigegeben.

[0045] Wird dagegen festgestellt, daß eine Übereinstimmung der Festcodes 1 und 2 vorliegt, so werden auch die Rolling Codes 1 und 2 von den Vergleichsmitteln 7 der Fahrzeugeinrichtung 1 miteinander verglichen.

[0046] Ergibt sich wiederum eine Übereinstimmung, so wird der Start direkt freigegeben. Hier handelt es sich um die "Normalfunktion". Eine spezielle weitere Reaktion seitens des Fahrzeugs ist nicht erforderlich.

[0047] Stimmt der von der Fernbedienung 2 übermittelte Rolling Code 2 jedoch nicht mit dem aktuellen Rolling Code 1 des Fahrzeugs überein, so kommen hierfür zwei mögliche Ursachen in Frage. Zum einen kann ein Unbefugter versuchen, das Freigabesystem zu überlisten. Zum anderen kann die Fernbedienung 2 zwar gültig, die Synchronisierung aber verloren gegangen sein, weil die Batterie ausgewechselt oder der Betätigungsknopf zu oft gedrückt wurde.

[0048] Um feststellen zu können, welche der Ursachen in Frage kommt, wird in dem Fall, daß sich ein Transponder 4 im Niederfrequenz-Sendefeld des Fahrzeugs, welches von den Sende/Empfangsmittel 9 erzeugt wird, befindet, eine Kommunikation aufgebaut, um festzustellen, ob der Transponder 4 gültig ist. Falls der Transponder 4 nicht gültig ist, so wird angenommen, daß die verwendete Fernbedienung 2 nicht zur Anforderung der Startfreigabe berechtigt ist, und der Vorgang wird abgebrochen. Ist der Transponder 4 jedoch gültig,

so wird angenommen, daß es sich um eine berechtigte und lediglich nicht mehr synchronisierte Fernbedienung 2 handelt, und zunächst die Alarmanlage entschärft und der Start freigegeben.

[0049] Anschließend wird entsprechend Figur 3 eine neue Synchronisierung zwischen Fahrzeug und Fernbedienung 2 durchgeführt.

[0050] Die Sende/Empfangsmittel 9 des Fahrzeugs senden zu diesem Zweck einen Header als Synchronisierungsbefehl an den Transponder 4 der Fernbedienung 2. Danach wird eine Zufallszahl von den Sende/Empfangsmittel 9 des Fahrzeugs an den Transponder 4 der Fernbedienung 2 gesandt. Sowohl Fahrzeug als auch Fernbedienung 2 verschlüsseln mit den jeweiligen Verschlüsselungsmitteln die Zufallszahl mit der Funktion f und mit der Funktion g. Eine Kombination aus den Ergebnissen der Berechnungen werden sowohl im Fahrzeug wie auch in der Fernbedienung 2 dazu verwendet, um den aktuellen Zustand des jeweiligen Rolling Code Generators 5,6 neu zu setzen. Dadurch laufen die beiden Maschinen wieder synchron und bei der nächsten Kommunikation kann die Startfreigabe wieder als "Normalfunktion" erfolgen.

25 Patentansprüche

1. Freigabesystem zur Überprüfung, ob eine Anforderung der Freigabe von Funktionen einer Einrichtung berechtigt ist, wobei die Funktionen beispielsweise in der Entschärfung einer Alarmanlage oder einer Wegfahrsperre und in der Aktivierung einer Zentralverriegelung eines Fahrzeugs bestehen können, mit einem einrichtungsseitig angeordneten ersten Generator (6) zum Erzeugen eines ersten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des ersten Generators (6), sowie mit einer Fernbedienung (2), die einen zweiten Generator (5) umfaßt zum Erzeugen eines zweiten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des zweiten Generators (5), Mittel (3) zum Übertragen des generierten zweiten Codes über eine Funkstrecke an die Einrichtung sowie einen Transponder (4), der geeignet ist, die Fernbedienung (2) gegenüber der Einrichtung zu authentifizieren, wobei der Generator (5) der Fernbedienung (2) und der Generator (6) der Einrichtung geeignet sind zur synchronen Generierung eines Codes und wobei dem einrichtungsseitigen ersten Generator (6) Vergleichsmittel (7) zugeordnet sind zum Vergleichen des einrichtungsseitig generierten und des in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes für eine Überprüfung der Berechtigung der Fernbedienung (2) zur Anforderung der Freigabe der Funktionen, dadurch gekennzeichnet, daß einrichtungsseitig Mittel (9) zum Bereitstellen eines Synchronisierungssignals sowie Ausgabe-

mittel (9) zum Übertragen des Synchronisierungssignals an den Transponder (4) der Fernbedienung (2) vorgesehen sind, wobei die Innenzustände der Code Generatoren (5,6) mittels des Synchronisierungssignals miteinander synchronisierbar sind.

2. Freigabesystem nach Anspruch 1, dadurch gekennzeichnet,

- daß einrichtungsseitig Verschlüsselungsmittel angeordnet sind zum Generieren eines Wertes für den Innenzustand des Code Generators (6) der Einrichtung aus mindestens einem Teil des bereitgestellten Synchronisierungssignals sowie Steuermittel zum Setzen des Innenzustandes entsprechend des generierten Wertes und
- daß die Fernbedienung (2) weitere Verschlüsselungsmittel aufweist zum Generieren eines Wertes für den Innenzustand des Code Generators (5) der Fernbedienung (2) basierend auf mindestens einem Teil des von dem Transponder (4) empfangbaren Synchronisierungssignals, und Steuermittel zum Setzen des Innenzustandes entsprechend des von den weiteren Verschlüsselungsmitteln generierten Wertes.

3. Freigabesystem nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet,

daß die von der Einrichtung bereitgestellten Synchronisierungssignale sich zusammensetzen aus einem Synchronisierungsbefehl zum Auffordern der Fernbedienung (2), neu zu synchronisieren, und aus einer Zufallszahl als zugrundezulegendem Wert für das Setzen des Innenzustandes des Code Generators (5,6) der Einrichtung sowie der Fernbedienung (2).

4. Freigabesystem nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet,

daß die Einrichtung und die Fernbedienung (2) jeweils Mittel aufweisen zum Speichern eines Festcodes, der bei jeder Freigabeanforderung zusammen mit dem aktuellen sich schrittweise ändernden Code von der Fernbedienung an die Einrichtung übertragen wird, und daß die Einrichtung Vergleichsmittel (7) aufweist zum Überprüfen der Identität eines über Funkstrecke empfangenen Festcodes mit dem für diese Fernbedienung (2) gespeicherten Festcode.

5. Freigabesystem nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet, daß die Code Generatoren (5,6) von der Fernbe-

dienung (2) und von der Einrichtung Generatoren zum Generieren eines Rolling Codes basierend auf einem in der Fernbedienung (2) und in der Einrichtung gespeicherten, identischen "secret key" sind.

6. Verfahren für ein Freigabesystem zur Überprüfung, ob eine Anforderung der Freigabe von Funktionen einer Einrichtung berechtigt ist, wobei die Funktionen beispielsweise in der Entschärfung einer Alarmanlage oder einer Wegfahrsperre und in der Aktivierung einer Zentralverriegelung eines Fahrzeugs bestehen können, mit einem einrichtungsseitig angeordneten ersten Generator (6) zum Erzeugen eines ersten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des ersten Generators (6), sowie mit einer Fernbedienung (2), die einen zweiten Generator (5) umfaßt zum Erzeugen eines zweiten, sich schrittweise ändernden Codes ausgehend von einem aktuellen Innenzustand des zweiten Generators (5), Mittel (3) zum Übertragen des generierten zweiten Codes über eine Funkstrecke an die Einrichtung sowie einen Transponder (4), der geeignet ist, die Fernbedienung (2) gegenüber der Einrichtung zu authentifizieren, wobei der Generator (5) der Fernbedienung (2) und der Generator (6) der Einrichtung geeignet sind zur synchronen Generierung eines Codes und wobei dem einrichtungsseitigen ersten Generator (6) Vergleichsmittel (7) zugeordnet sind zum Vergleichen des einrichtungsseitig generierten und des in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes für eine Überprüfung der Berechtigung der Fernbedienung (2) zur Anforderung der Freigabe der Funktionen, und wobei das Verfahren die folgenden Schritte umfaßt:

- Senden eines Synchronisierungsbefehls, insbesondere eines Headers, von der Einrichtung an den Transponder (4) der Fernbedienung (2) zum Signalisieren, daß neu synchronisiert werden soll,
- Senden einer in der Einrichtung generierten Zufallszahl von der Einrichtung an den Transponder (4) der Fernbedienung (2), und
- Speichern eines auf der Zufallszahl basierenden Wertes als aktuellen Innenzustand der beiden Generatoren (5,6) in Einrichtung und Fernbedienung (2).

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet,

daß die Zufallszahl vor der Verwendung für das Setzen der aktuellen Innenzustände der beiden Generatoren (5,6) in der Einrichtung und in der Fernbedienung (2) mit mindestens einer, in Einrichtung und Fernbedienung (2) gleichen

Verschlüsselungsfunktion verschlüsselt wird.

1. Verfahren nach Anspruch 6 oder 7,
dadurch gekennzeichnet,

daß es nach jeder Freigabe der Funktionen der Einrichtung aufgrund einer Authentifizierung der Fernbedienung (2) durch den Transponder (4) nach nicht erfolgter Freigabe aufgrund des Vergleichs eines in der Einrichtung generierten Codes und eines in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes durchgeführt wird.

2. Verfahren nach Anspruch 6 oder 7,
dadurch gekennzeichnet,

daß es nach jeder Freigabe der Funktionen der Einrichtung aufgrund des Vergleichs eines in der Einrichtung generierten Codes und eines in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes durchgeführt wird.

3. Verfahren nach Anspruch 6 oder 7,
dadurch gekennzeichnet,

daß es nach jeder Freigabe der Funktionen der Einrichtung aufgrund des Vergleichs eines in der Einrichtung generierten Codes und eines in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes durchgeführt wird, sowie nach jeder Freigabe der Funktionen der Einrichtung aufgrund einer Authentifizierung der Fernbedienung (2) durch den Transponder (4) nach nicht erfolgter Freigabe aufgrund des Vergleichs eines in der Einrichtung generierten Codes und eines in der Fernbedienung (2) generierten und zu der Einrichtung übertragenen Codes.

4. Verfahren nach einem der Ansprüche 6 - 10, bei dem die Generatoren (5,6) von der Einrichtung und von der Fernbedienung (2) Rolling Codes erzeugen und bei dem von der Fernbedienung (2) für eine Freigabeanforderung zusammen mit dem generierten Rolling Code ein Festcode, für den in der Einrichtung und in der Fernbedienung (2) ein identischer Wert gespeichert ist, über Funkstrecke an die Einrichtung übertragen wird und bei dem die Freigabe der Funktionen durch Codevergleich bzw. durch Authentifizierung über den Transponder die folgenden Schritte umfaßt:

a) Überprüfen in der Einrichtung, ob ein Signal über Funkstrecke empfangen wurde;
b) falls ja in Schritt a), Überprüfen in der Einrichtung, ob ein empfangener Festcode mit

einem gespeicherten Festcode übereinstimmt;
c) falls ja in Schritt b), Überprüfen in der Einrichtung, ob ein empfangener Rolling Code mit einem in der Einrichtung generierten Rolling Code übereinstimmt;
d) falls ja in Schritt c), Freigabe der Einrichtungsfunktionen;
e) falls nein in Schritt c), Überprüfen in der Einrichtung, ob eine daraufhin veranlaßte Authentifizierungsaufforderung an den Transponder (4) der Fernbedienung (2) einen gültigen Transponder (4) ergibt;
f) falls ja in Schritt e), Freigabe der Einrichtungsfunktionen.

5. Verfahren nach einem der Ansprüche 6 - 11,
dadurch gekennzeichnet,
daß die Authentifizierung der Fernbedienung (2) über den Transponder (4) die folgenden Schritte aufweist:

- Senden einer Zufallszahl unverschlüsselt und mit einer ersten Funktion verschlüsselt von der Einrichtung an die Fernbedienung (2),
- Empfangen der unverschlüsselten und der verschlüsselten Zufallszahl durch den Transponder (4) der Fernbedienung (2),
- Verschlüsseln der unverschlüsselt empfangenen Zufallszahl mit einer ersten Funktion in dem Transponder (4),
- Überprüfen durch Transponder (4), ob die verschlüsselt empfangene Zufallszahl mit der unverschlüsselt empfangenen verschlüsselten Zufallszahl übereinstimmt,
- falls ja, Verschlüsseln der Zufallszahl mit einer zweiten Funktion und Zurücksenden an die Einrichtung und
- Überprüfen in der Einrichtung, ob die empfangene verschlüsselte Zufallszahl mit der in der Einrichtung mit der zweiten Funktion verschlüsselten Zufallszahl übereinstimmt.

6. Verfahren nach einem der Ansprüche 6-12,
dadurch gekennzeichnet,
daß für eine angeforderte Freigabe der Einrichtungsfunktionen der von einer Fernbedienung (2) generierte und gesendete Code in der Einrichtung verglichen wird mit einem Empfangsfenster, das eine vorgegebene Anzahl von in der Einrichtung generierten, aufeinanderfolgenden Codes umfaßt.

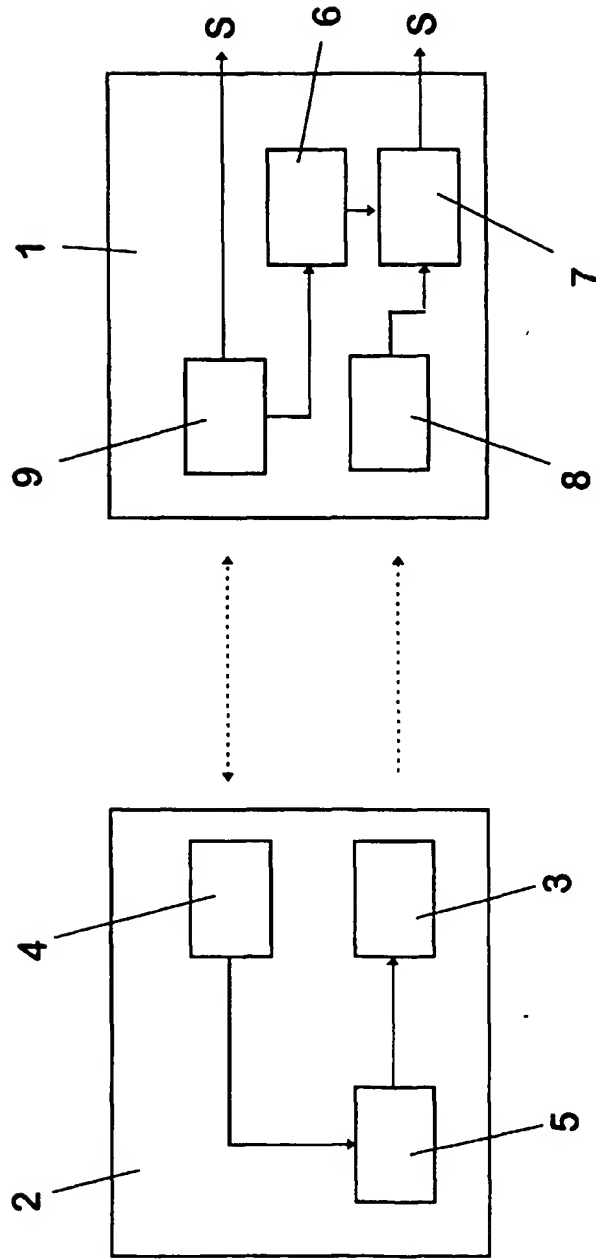


FIG. 1

Fahrzeug

Fernbedienung

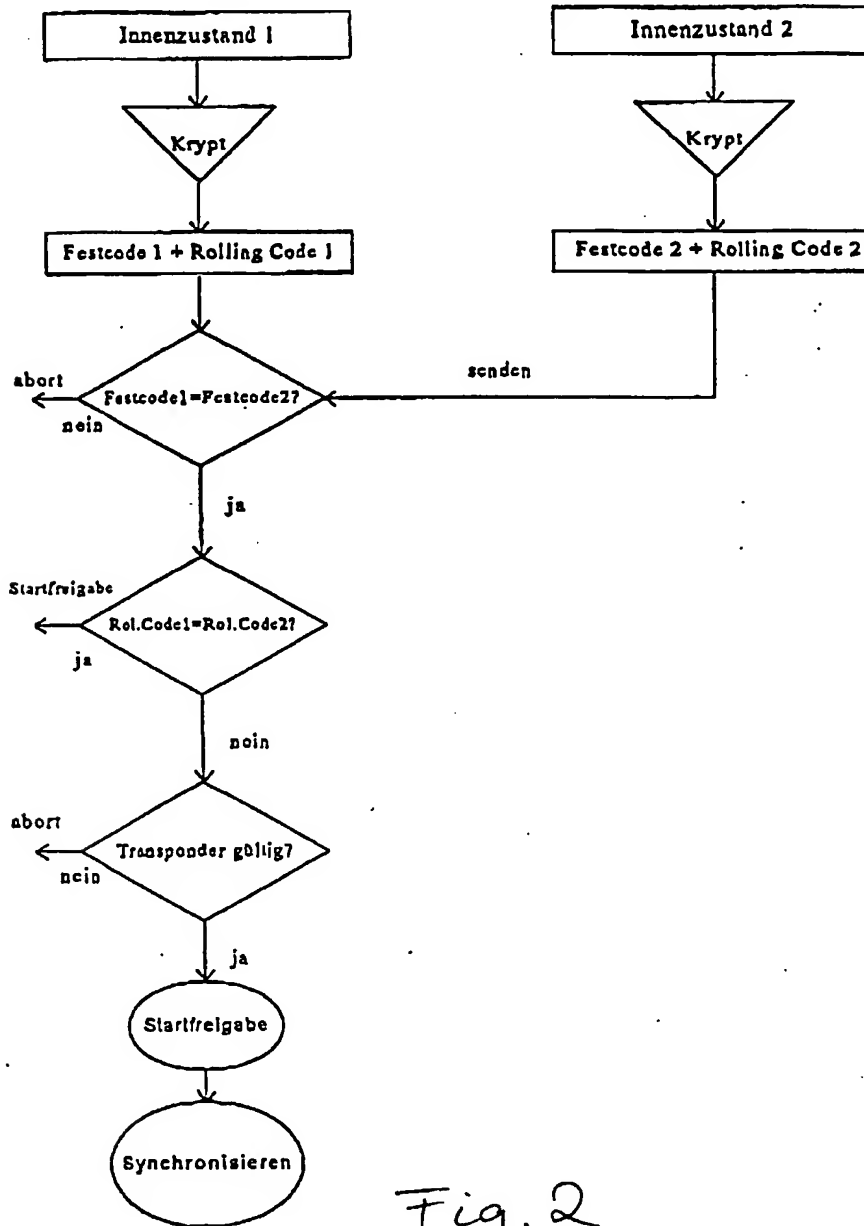


Fig. 2

Synchronisierung

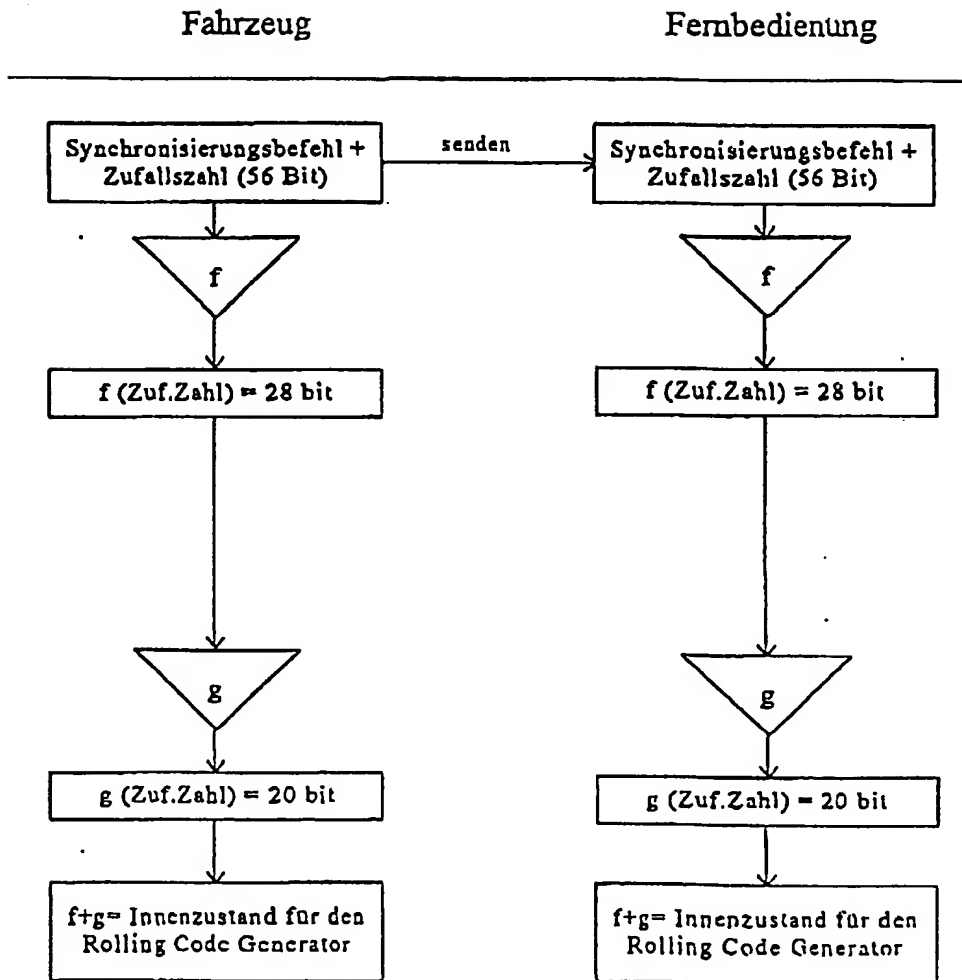


Fig 3



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EINSCHLÄGIGE DOKUMENTE			EP 99100358.3
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl. 6)
Y	US 5369706 A (LATKA, D.S.) 29. November 1994 (29.11.94), Spalte 3, Zeile 6 - Spalte 5, Zeile 60, Ansprüche. --	1-13	E 05 B 49/00
Y, P	DE 4428947 C1 (KIEKERT AG) 04. April 1996 (04.04.96), ganzes Dokument. --	1-13	
A	US 5646996 A (LATKA, D.S.) 08. Juli 1997 (08.07.97), Spalte 2, Zeile 19 - Spalte 5, Zeile 4. ----	1-13	
			RECHERCHIERTE SACHGEBIETE (Int. Cl. 6)
			E 05 B B 60 R H 04 L H 04 K
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.			
Recherchenort WIEN		Abschlußdatum der Recherche 07-05-1999	Prüfer SCHLECHTER
<p>KATEGORIE DER GENANNTEN DOKUMENTEN</p> <p>X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur T : der Erfindung zugrunde liegende Theorien oder Grundsätze</p> <p>E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus andern Gründen angeführtes Dokument A : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument</p>			

EP Form 1503 03 82

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 99100358.3

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patendokumente angegeben.
 Die Angaben über die Familienmitglieder entsprechen dem Stand der EPIDOS-INPADOC-Datei am 17. 5.1999.
 Diese Angaben dienen zur Unterrichtung und erfolgen ohne Gewähr.

Im Recherchenbericht angeführtes Patendokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US A 5369706	29-11-1994	CN A 1134178	23-10-1996
		DE CO 69408399	09-10-1997
		DE T2 69408399	09-10-1997
		EP A1 7193370	03-02-1998
		EP B1 7193370	03-09-1999
		JG T3 2107392	16-11-1997
		JP T2 9505657	10-06-1997
DE C1 4428947	04-04-1996	WO A1 9512733	11-05-1995
		DE A1 19533195	13-03-1997
		FR A1 2723759	13-02-1996
		FR B1 2723759	10-09-1997
		IT AO MI 9513232	20-06-1998
		IT A1 MI 1374756	16-12-1999
		IT B1 MI 1374756	08-11-1999
		JP A2 8193444	20-07-1996
		US A 55361420	01-10-1996
		US A 5774060	30-06-1998
		FR A1 2738587	14-03-1997
		IT AO MI 961394	05-07-1998
		IT A1 MI 961394	05-01-1999
		IT B1 MI 961394	21-11-1999
		JP A2 9170365	30-06-1997
US A 5646996	08-07-1997	CN A 1134206	23-10-1996
		EP A1 727117	21-08-1996
		JP T2 9504925	13-05-1997
		WO A1 9512940	11-05-1995

Bezüglich näherer Einzelheiten zu diesem Anhang siehe Amtsblatt des Europäischen Patentamtes, Nr. 12/82.